

REMARKS

The Examiner is thanked for the courteous telephone interview granted Applicant's representative on February 20, 2004. This Amendment has been drafted to respond to comments made by the Examiner during the interview; and, it is believed, places the application in condition for allowance.

The specification has been amended to correct a typographical error noted therein. No new matter has been added by the amendment.

Claims 1-40 remain pending in the present application. Claims 4, 5, 15, 16, 25, 26 and 39 have been amended. No claims have been added. Applicant believes the claims currently in the case patentably distinguish over the cited art, and that this application is now in condition for allowance. Reconsideration of the rejection is, accordingly, respectfully requested in view of the above amendments and the following comments.

I. 35 U.S.C. § 112, Second Paragraph

The Examiner has rejected claims 4, 5, 15, 16, 25, 26 and 29 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In particular, the Examiner has objected to the phrase "and/or" in those claims as being unclear.

By the present Amendment, the alternative language of the claims has been deleted and replaced by the phrase "at least one of files and resources". This terminology is believed to be clear and definite in all respects, and to fully satisfy the requirements of 35 U.S.C. 112, second paragraph.

Therefore, the rejection of claims 4, 5, 15, 16, 25, 26 and 29 under 35 U.S.C. § 112, second paragraph, has been overcome and withdrawal of the rejection is respectfully requested.

II. 35 U.S.C. § 102, Anticipation

The Examiner has rejected claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35 and 37-40 under 35 U.S.C. § 102(e) as being anticipated by Glasser et al. (U.S. Patent No. 5,956,715). This rejection is respectfully traversed.

Glasser et al. (hereinafter Glasser) discloses a technique for managing file and other resource security in a networked computing environment. The network includes server computers, each of which controls a particular resource that is shareable among users of the network. A resource may be organized as a hierarchy of elements, and a procedure is described for changing security protection; e.g., access authorization, to an element in the hierarchy.

The present invention is directed to a procedure by which the security configuration of a plurality of servers can be updated from a centralized server. As shown in Figure 1 of the present application, a directory server 150 can download updates of security configurations to each of a plurality of servers 120, 130 and 140, thus making it unnecessary to separately change the security configuration at each of the plurality of servers.

In rejecting the claims, the Examiner states the following:

Glasser et al. discloses a method of updating security configurations of a plurality of servers, comprising:

- Changing security information in a centralized server, where the security information is the commands for manipulating resource access permissions (Column 7, lines 45-48)
- Receiving an update command (Column 7, lines 46-48)
- Downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed security information is used to update the security configurations of the plurality of servers, where the downloaded information occurs when the security information is propagated down the network (Column 7, lines 60-65)

Office Action dated February 4, 2004, page 3.

Claim 1 of the present application reads as follows:

1. A method of updating security configurations of a plurality of servers, comprising:
changing security information in a centralized server;
receiving an update command; and
downloading the changed security information to the plurality of servers in response to receiving the update command, wherein the downloaded changed

security information is used to update the security configurations of the plurality of servers.

Glasser does not disclose changing security information in a centralized server. Instead, Glasser generally discloses changing security information for a particular server at the server. For example, in Col. 7, lines 46-48, Glasser states that when changing access permission to a resource controlled by peer server 120, "[c]ommands for manipulating resource access permissions are assumed to be received from user interface 125 of peer server 120". Thus, security information is not changed in a centralized server but is changed at server 120 itself via GUI 125 associated with the server.

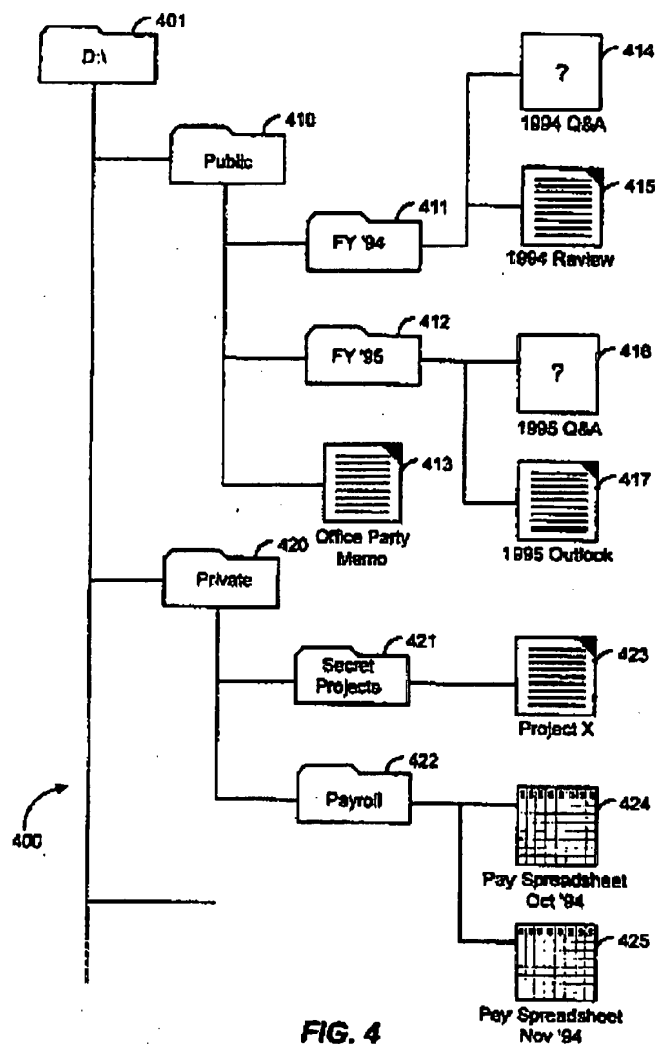
Although, as pointed out by the Examiner, the commands can also come from a remote source or from another node of the network (col. 7, lines 48-54 of Glasser), the change in access information for the resource stored in hard disk 121 is still being made in peer server 120 and not from a centralized server.

Glasser also does not disclose downloading changed security information to a plurality of servers in response to an update command. Again, in Glasser, security information appears to be downloaded to a resource associated with a particular server from that particular server, not to a plurality of servers in response to an update command.

Accordingly, in Glasser, there is no centralized server in which security information is changed, and no downloading of changed security information to a plurality of servers (such as, for example, peer servers 120 and 140 in Glasser). In Glasser, security information is changed at each server.

During the above-mentioned telephone interview, the Examiner pointed out that files stored on hard disk 121 associated with peer server 120 are arranged in a hierarchical manner, and that Glasser could, perhaps, be construed as reading on claim 1 by virtue of changed security information being downloaded through the hierarchy, Applicant respectfully disagrees.

Figure 4 of Glasser is as follows:



As shown in Figure 4 of Glasser, hierarchy 400 comprises a plurality of files and folders 401, 410, 411, etc., stored on hard disk 121 associated with peer server 120. Some of the files and folders have an access control list (ACL), while other folders and files inherit an ACL from the nearest ancestor folder or file having an ACL.

In Column 7, lines 55-58, Glasser reads:

“Initially, the resource for which permissions are to be established or modified is selected (step A). Peer server 120 receives a command to change the permissions for the selected resource (step B).”

In Glasser, peer server 120 receives a command to change the permissions for a selected resource. Peer server 120 then determines if the resource, e.g., a particular folder, has its own ACL. If so, the folder's own ACL is updated. If not, the nearest ancestor having an ACL is determined, and that ACL is updated.

Thus, even if the files and folders stored in hard disk 121 can be considered as being “servers”, which Applicant does not believe to be the case, security information is still being changed only in a particular ACL for a folder or file, and changed security information is not downloaded from a centralized server to a plurality of servers in response to receiving an update command as recited in claim 1.

For at least all the above reasons, Glasser does not anticipate Claim 1, and withdrawal of the rejection thereunder is respectfully requested.

Claims 2-6, 8 and 10 depend from and further restrict claim 1 and are also not anticipated by Glasser, at least by virtue of their dependency. Many of these claims, however, recite additional features not disclosed in Glasser. For example, with respect to claims 2 and 3, inasmuch as Glasser fails to disclose a centralized server, it also fails to disclose a directory server as a centralized server, or using an editor to change a directory listing in a centralized server.

Independent claim 12 recites a controller and a storage device coupled to the controller. In addition, claim 12 recites that the controller, in response to receiving an update command, downloads security information stored in the storage device to a plurality of servers via a network interface. Claim 12 is not anticipated by Glasser for reasons similar to those discussed above with respect to claim 1, and claim 12, together with claims 13-17, 19, 21 and 22 dependent thereon, are also believed to be allowable in their present form.

In addition, for reasons similar to those discussed above with respect to claim 1, independent claims 23, 32 and 37 are also not anticipated by Glasser, and should be

allowable in their present form, together with claims 24-27, 29, 31, 33, 35 and 38-40 dependent thereon.

The claims would also not be obvious in view of Glasser. As discussed above, Glasser does not disclose changing security information in a centralized server, nor does the reference disclose downloading changed security information to a plurality of servers in response to receiving an update command. Only the present application contains such a disclosure. In the absence of any such disclosure in Glasser, it would not be obvious to a person of ordinary skill in the art to modify Glasser to achieve the present invention.

Therefore, the rejection of claims 1-6, 8, 10-17, 19, 21-27, 29, 31-33, 35 and 37-40 under 35 U.S.C. § 102 has been overcome.

III. 35 U.S.C. § 103, Obviousness

The Examiner has rejected claims 7, 9, 18, 20, 28, 30, 34 and 36 under 35 U.S.C. § 103(a) as being unpatentable over Glasser. In rejecting these claims, the Examiner takes official notice that receiving update commands at scheduled periodic times is well-known to those of ordinary skill in the art; and, further, that lightweight directory access protocol (LDAP) is well known to those of ordinary skill in the art.

These claims all depend from and further restrict independent claims. The matters of which the Examiner takes official notice do not supply the deficiencies in Glasser with respect to the independent claims, as discussed above; and for at least the reasons discussed above, claims 7, 9, 18, 20, 28, 30, 34 and 36 are not obvious in view of Glasser, and should be allowable in their present form.

Therefore, the rejection of claims 7, 9, 18, 20, 28, 30, 34, and 36 under 35 U.S.C. § 103 has been overcome.

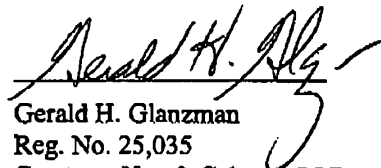
IV. Conclusion

For all the above reasons, it is submitted that claims 1-40 are allowable in their present form, and that this application is now in condition for allowance. It is, accordingly, respectfully requested that the Examiner so find and issue a Notice of Allowance in due course.

The Examiner is invited to call the undersigned at the below-listed telephone number if, in the opinion of the Examiner, such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: February 26, 2004

Respectfully submitted,



Gerald H. Glanzman
Reg. No. 25,035
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Attorney for Applicant